

# INDIANA STATE POLICE

## IDENTITY THEFT- REDUCING YOUR RISK

Identity theft is the fastest growing crime of the 21<sup>st</sup> century and occurs when someone wrongfully uses your personal information to obtain credit, loans, rentals, mortgages, cell phones or utilities in your name. They may also commit traffic offences or crimes while impersonating you.

Becoming a victim of identity theft is an experience you will never forget. It is an overwhelming event that you may not find out about for months or years, and when you do, it can take weeks or months to recover, with an average out-of-pocket expense of \$1,200 or more.

The Federal Trade Commission (FTC) released a report in November of 2007, indicating 8.3 million U.S. residents were victims of identity theft in 2005. Losses to more than half of the victims were \$500 or less and \$6,000 or more in 10 percent of the cases, with an average loss of \$1,882. For the criminal, identity theft is a low risk, high reward crime considering that the average take in an armed robbery is less than two hundred dollars compared to thousands in identity theft.

Identity theft crosses all social, economic, racial and gender barriers. The suspect could be a relative, dishonest employee, someone you know or have never met. They could live next door, across the country, around the world or surf the Internet leaving a confusing paper trail behind them. The suspects will empty savings, checking, investment and credit card accounts.

Electronic technology has made our lives easier but also has made stealing information more convenient for the identity thieves; trading convenience for security may not be the right decision when conducting business. Is there really such a thing as a *secured site*? Think about it.

You may take all measures to protect yourself, but still could become a victim through public access records that are available in local, state and federal governmental agencies. Many identity theft cases can be tracked back to the suspect obtaining information or identification documents through these offices. These government agencies are taking a hard look at their security measures currently in place and are making corrections.

It is impossible to completely prevent identity theft. Education and common sense can reduce your risk from becoming a victim – here are a few helpful hints:

- Release SSN and birth date only when absolutely necessary. Ask, “Why do you want it and what are you going to do with it”?
- Do not have SSN printed on checks or your BMV documents including driver’s license or I.D. card.

- Review SSN benefits statement once a year to check for fraud. If your SSN is fraudulently used, report it to the Social Security Fraud Hotline at (800)-269-0271.
- Reduce the number of credit cards you use. Cancel all unused accounts and destroy the old cards. Keep a list/photocopy of credit card information, including telephone numbers of customer service departments in a secure location.
- Cross-shred pre-approved credit applications, credit card receipts, bills and other financial documents.
- Order your **FREE** credit report once a year from the three credit reporting companies at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) Check the report for inaccuracies and fraudulent use of accounts. Equifax (800)-997-2493, Experian (888)-397-3742, and TransUnion (800)-916-8800. **Space them out, one every four months.**
- Research installing a “freeze” on you credit reports by visiting the Indiana Attorney General’s web site at [www.IndianaConsumer.com](http://www.IndianaConsumer.com)
- Reduce pre-approved credit card applications (888)-567-8688 to remove your name for two years or permanently.
- Reduce unwanted junk mail; write to Direct Marketing Association’s Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735-9008.
- Register for Indiana’s Telephone Privacy List (888)-834-9969.
- When dialing a phone number, your name, address and number may be captured. Dial \*67 before your initial call. This is a free service provided by **most** phone companies and it blocks caller I.D. Put a caller I.D. block on your cell phone.
- Do not give personal information on cordless or cell phones. Your conversation can be picked up by scanners and baby monitors.
- Never use SSN, birth dates, or maiden names for PIN codes.
- Never let credit or debit cards out of your sight or loan them to anyone. Put daily withdrawal limits on your cards. Be cautious of self-serve swipe devices, the magnetic strip information can be pick-up by receiving devices hooked to laptop computers.
- Encourage businesses to check for I.D. when accepting cashing checks or credit cards and to destroy documents properly.

**If you are a victim, immediately:**

- Insist on a police report, no matter where the crime occurred. You need a case or incident number to proceed.
- Call the credit reporting bureaus, banks and creditors to put a “Fraud Alert” on your accounts.
- Contact the Federal Trade Commission (FTC) (877)-ID-THEFT or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) for victim assistance and affidavits.
- Start the recovery process.